

# Secrecy Outage Probability of Network-Coded Cooperative Communication

João Luiz Rebelatto, *Member, IEEE*, Richard Demo Souza, *Senior Member, IEEE*,  
Rodrigo Tsuneyoshi Kaido, *Ohara Kerusauskas Rayel, Student Member, IEEE* and  
Bartolomeu F. Uchôa-Filho, *Senior Member, IEEE*

**Abstract**—We evaluate the secrecy performance of a multiple access cooperative network where the destination node is wiretapped by a malicious and passive eavesdropper. We propose the application of the network coding technique as an alternative to increase the secrecy at the destination node, on the top of improving the error performance of the legitimate communication, already demonstrated in the literature. Network coding is leveraged by assuming that the legitimate cooperative nodes are able to perform non-binary linear combinations of different frames before the transmission. Different scenarios with and without channel state information (CSI) at the transmitter side are evaluated. The effectiveness of the proposed schemes is evaluated in terms of secrecy outage probability through theoretic and numerical analyses. It is shown that, even when the legitimate transmitters do not have any CSI, the secrecy can be increased through the use of network coding when compared to the direct transmission and traditional cooperative techniques.

**Index Terms**—Cooperative communications, network coding, wiretap channel, secrecy outage probability.

## I. INTRODUCTION

Information security has become a major concern in wireless communications, due to the broadcast nature of the wireless medium which allows eavesdroppers to potentially intercept any transmission. Information theoretic secrecy, introduced by Shannon in 1949 [1], is a promising approach towards increasing communication security. In [2], Wyner elaborated on the work of Shannon by introducing the so-called wiretap channel, which is composed of a pair of legitimate nodes communicating in the presence of an eavesdropper.

Recent works have applied information theoretic secrecy ideas to wireless communications, showing that the randomness inherent to wireless channels can help in improving the secrecy of the network [3]–[7], under different assumptions regarding channel state information (CSI) at the transmitters. When the transmitters have global CSI regarding the legitimate and eavesdropper links, perfect secrecy is achieved by adapting the rate of the wiretap code [3]. When only the CSI of the legitimate channels are available at the transmitter side, as commonly assumed in the literature [4], [5], [8]–[12], the secrecy needs to be evaluated through a probabilistic analysis, by finding the probability that the information is leaked to the

eavesdropper for a given fixed secure transmission rate. The problem of establishing secure communication in a scenario without any CSI at the transmitter side was also addressed in the literature [6], [7]. In this situation, the secrecy outage probability becomes the union of two independent events: *i.*) the *reliability outage event*, when the legitimate receiver could not decode the transmitted message; and *ii.*) the *secrecy outage event*, when the instantaneous capacity of the eavesdropper is above the equivocation rate of the considered wiretap code.

Similarly to communication networks without secrecy constraints, the channel conditions dictate the network performance. It is then necessary for the legitimate nodes to have some advantage over the eavesdropper in terms of instantaneous channel quality to guarantee the existence of secure communications. In this regards, many techniques have been recently proposed to increase the secrecy in wireless networks. Some of them consider the use of multiple antennas [8], [9], or even adopt the concept of cooperative communications [10]–[12], which is a technique initially proposed to increase the reliability of wireless communications [13], [14]. In cooperative networks, the sources help each other by relaying their messages, and the transmission is usually divided in two phases: the so-called *broadcast phase* (BP), where the sources broadcast their own information frames (IFs), and the *cooperative phase* (CP), where the nodes transmit parity frames (PFs) to the destination, which are composed of redundant information related to their own IFs and/or to the IFs of their partners. One of the most well known cooperative protocols is the decode-and-forward (DF) [13], where the nodes just act as routers in the cooperative phase, relaying the IF from its partner.

In [11], the authors presented a pioneering study on the secrecy of cooperative communications, by combining concepts of the relay [15] and wiretap [2] channels in the so-called relay-eavesdropper channel, as well as establishing the theoretical bounds for the rate-equivocation of the channel. More recently, the secrecy performance of a cooperative network under the DF protocol was carried out in [10], considering either a passive or an active eavesdropper. It was shown in [10] that cooperation is capable of increasing the network secrecy when compared to the direct transmission.

The network coding technique [16] has been also recently applied to cooperative networks, aiming to increase their reliability [17], [18]. In a network-coded cooperative network, the sources transmit linear combinations of different messages instead as just acting as routers. It was shown in [17], [18] that,

This work has been supported in part by CNPq and CAPES, (Brazil).

João Luiz Rebelatto, Richard Demo Souza, Rodrigo Tsuneyoshi Kaido and Ohara Kerusauskas Rayel, are with the CPGEI, Federal University of Technology - Parana, Curitiba, PR, 80230-901, Brazil (e-mail: {jlrebelatto, richard}@utfpr.edu.br, rodrigokaido@gmail.com, oharakr@gmail.com).

Bartolomeu F. Uchôa-Filho is with the EEL, Federal University of Santa Catarina, Florianópolis, SC, 88040-900, Brazil (e-mail: uchoa@eel.ufsc.br).

if such linear combinations are performed over a large enough non-binary finite field  $\text{GF}(q)$ , the system diversity order can be increased when compared to the traditional DF protocol, reducing the system outage probability.

Motivated by the promising performance of the network coding technique, we presented in [12] some preliminary results on the performance of such technique in a scenario subject to secrecy constraints, where two sources aim to cooperatively transmit independent information to a common destination in the presence of a malicious eavesdropper. The results in [12], which assumes CSI of the legitimate channels at the transmitters, indicate the potential of network coding to increase the secrecy.

### A. Contributions

Against the background presented above, the novel contributions of this paper are summarized as follows:

- We elaborate on the results from [12] by extending in time the code construction, allowing the sources to transmit an arbitrary and independent number of frames either in the broadcast or the cooperative phase. More specifically, we adopt the generalized network coding (GNC) scheme from [18] instead of the network coding scheme from [17] adopted in [12];
- We also generalize the results in [12] to a network-coded cooperative network with multiple ( $M \geq 2$ ) sources, obtaining closed-form approximations to the secrecy outage probability under the assumption that the sources have CSI of the legitimate channels, but do not know the channel to the eavesdropper, as commonly assumed in the literature;
- Since even partial CSI is not easy to be obtained in practice, we also calculate the secrecy outage probability of the network-coded cooperative scheme in the situation where the sources do not have any CSI at all, and show that even in this case network coding can be beneficial towards increasing the network secrecy.

The rest of this work is organized as follows. In Section II we introduce the system model, while Section III introduces the concept of secrecy outage probability considering the direct non-cooperative communication. Sections IV and V present the DF and GNC cooperative protocols, respectively. The secrecy outage analysis of the GNC scheme is carried out in Section VI, which is followed by numerical results in Section VII. Finally, Section VIII concludes the paper.

*Notations:*  $\log(\cdot)$  denotes base-2 logarithm.  $(x)^+$  means  $\max\{0, x\}$ . Lower-case boldface symbols represent vectors. The symbol  $\boxplus$  stands for summation over a finite field  $\text{GF}(q)$ .

## II. SYSTEM MODEL

We consider a multiple access cooperative network composed of  $M$  sources having independent information to transmit to a common destination node. We assume the existence of a malicious eavesdropper (also referred to as just E) near the destination node, as illustrated in Fig. 1. Omitting the time

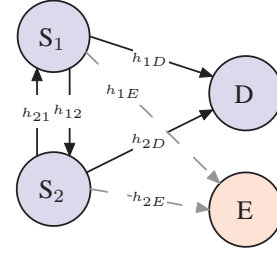


Fig. 1. System model. Multi-source network where nodes (two in the example, referred to as  $S_1$  and  $S_2$ ) have independent information to transmit to a common destination (D) in the presence of an eavesdropper (E).

index, the signal received by node  $j$  after a transmission of signal  $\mathbf{x}_i$  performed by source  $i$  is given by

$$\mathbf{y}_j = \sqrt{P_i d_{ij}^{-\alpha}} h_{ij} \mathbf{x}_i + \mathbf{n}_j, \quad (1)$$

where  $P_i$  corresponds to the transmission power,  $d_{ij} > 1$  represents the distance between sources  $i$  and  $j$ ,  $\alpha$  stands for the path-loss exponent,  $h_{ij}$  represents the block-fading coefficient, modeled as a circularly-symmetric complex Gaussian independent and identically distributed random variable (thus  $|h_{ij}|$  follows a Rayleigh distribution). The additive white Gaussian noise is represented by  $\mathbf{n}_j$  and we assume unitary bandwidth.

We adopt the notation  $i, j \in \{1, \dots, M, D, E\}$  when referring to source 1 ( $S_1$ ) to source  $M$  ( $S_M$ ), destination (D) and eavesdropper (E), respectively. The instantaneous signal-to-noise ratio (SNR) is defined as

$$\gamma_{ij} = \bar{\gamma}_{ij} |h_{ij}|^2, \quad (2)$$

where  $\bar{\gamma}_{ij} = \frac{P_i}{d_{ij}^\alpha \sigma_j^2}$  is the average SNR and  $\sigma_j^2$  is the noise variance. We assume a symmetric scenario in which all source nodes are approximately at the same distance from D; then  $\bar{\gamma}_{iD} = \bar{\gamma}_D \forall i \in \{1, 2, \dots, M\}$ . Moreover, we also assume that all sources are at approximately the same distance from E, so that  $\bar{\gamma}_{iE} = \bar{\gamma}_E \forall i \in \{1, 2, \dots, M\}$ .

Without secrecy constraints, assuming Gaussian inputs, an outage event in an individual link occurs when the mutual information  $\mathcal{I} = \log(1 + \gamma)$  falls below a given target information rate  $\mathcal{R}$  (in bits/channel use). The probability of such an event is called *outage probability*, and is defined as [19]

$$\begin{aligned} \mathcal{O}(\mathcal{R}, \bar{\gamma}) &\triangleq \Pr\{\mathcal{I} < \mathcal{R}\} \\ &= \Pr\left\{|h|^2 < \frac{2^{\mathcal{R}} - 1}{\bar{\gamma}}\right\}. \end{aligned} \quad (3)$$

One can see that the definition of outage probability presented in (3) corresponds to the cumulative density function (CDF) of the random variable  $|h|^2$  evaluated at the point  $(2^{\mathcal{R}} - 1)/\bar{\gamma}$ . As  $|h|$  follows a Rayleigh distribution, then  $|h|^2$  is exponentially distributed and the outage probability in (3) becomes [19]

$$\mathcal{O}(\mathcal{R}, \bar{\gamma}) = 1 - \exp\left(-\frac{2^{\mathcal{R}} - 1}{\bar{\gamma}}\right). \quad (4)$$

Based on the formulation of the individual link outage probability, under the assumption that all the links throughout the

network are subject to independent and identically distributed Rayleigh fading, the overall outage probability of a generic scheme  $X$  can be approximated for high SNR region as [18]

$$\begin{aligned}\tilde{\mathcal{O}}_X(\mathcal{R}, \bar{\gamma}) &= \mu_X [\mathcal{O}(\mathcal{R}, \bar{\gamma})]^{\mathcal{D}_X} \\ &= \mu_X \left[ 1 - \exp\left(-\frac{2^{\mathcal{R}} - 1}{\bar{\gamma}}\right) \right]^{\mathcal{D}_X},\end{aligned}\quad (5)$$

where  $\mu_X$  and  $\mathcal{D}_X$  correspond to the *coding gain* and *diversity order* of scheme  $X$ , respectively. Moreover, the diversity order  $\mathcal{D}_X$  is formally defined as [19]

$$\mathcal{D}_X \triangleq \lim_{\bar{\gamma} \rightarrow \infty} \frac{-\log \mathcal{O}_X(\mathcal{R}, \bar{\gamma})}{\log \bar{\gamma}}. \quad (6)$$

In order to perform a fair comparison between different protocols, one must take into account the multiplexing loss inherent to many cooperative schemes [13]. Thus, we consider that the target information rate of the generic cooperative protocol  $X$  is given by  $\mathcal{R}_X \triangleq \mathcal{R}/R_X$ , where  $\mathcal{R}$  is the attempted transmission rate in the case of non-cooperative direct transmission, and  $R_X$  corresponds to the code rate of the protocol  $X$ , defined as the ratio between the number of time slots allocated to the transmission of new data and the total number of time slots used by the protocol, with  $0 \leq R_X \leq 1$ . For the direct transmission,  $R_X = R_{DT} = 1$ .

### III. SECRECY OUTAGE PROBABILITY (SOP)

In the case where the sources have global channel state information (CSI), as in [3], perfect secrecy can be achieved by adapting the rate of the wiretap code according to the instantaneous channels realization (seen at both the legitimate and the eavesdropper). However, since assuming the knowledge of instantaneous channel condition of the eavesdropper might not be practical in several cases, in what follows we evaluate two more realistic scenarios regarding the availability of CSI at the source nodes: *i)* The sources have CSI of the legitimate channels only; *ii)* The sources have no CSI at all.

#### A. Sources with partial CSI

When only the CSI of the legitimate links is available at the sources, perfect secrecy cannot be guaranteed since the instantaneous channel information from E is unknown. Thus, a probabilistic secrecy analysis must be carried out [4], by determining the probability that E successfully spies some amount of information, for a given fixed secure transmission rate (which implies a variable transmission rate over the legitimate channel following its instantaneous capacity). It is noteworthy that this is the scenario assumed in most papers addressing secrecy outage probability in the literature, as for instance [4], [8], [9].

More specifically, following the wiretap code construction described for instance in [5], if we assume that the channel condition of the legitimate destination is known at the sources, we can design a wiretap code with block length  $n$  that contains  $2^{n\mathcal{R}}$  codewords, where the transmission rate  $\mathcal{R}$  is made equal to  $\mathcal{C}_D$ , the instantaneous channel capacity seen at the legitimate destination. Moreover, we set a number of codewords per bin in the wiretap code equal to  $2^{n\mathcal{R}_E}$ , where

$\mathcal{R}_E$  is the eavesdropper's equivocation rate. The rate of secure communication is then  $\mathcal{R}_s = \mathcal{R} - \mathcal{R}_E = \mathcal{C}_D - \mathcal{R}_E$ , which is usually fixed, implying that  $\mathcal{R}_E = \mathcal{C}_D - \mathcal{R}_s$  varies according to the channel condition seen at the legitimate destination.

Therefore, a secrecy outage event occurs when the instantaneous eavesdropper's channel capacity,  $\mathcal{C}_E$ , exceeds the equivocation rate  $\mathcal{R}_E$ , or alternatively when the difference between the instantaneous capacities of the main and the eavesdropper channels  $\mathcal{C}_D - \mathcal{C}_E$  is lower than  $\mathcal{R}_s$  [5]. Considering Gaussian inputs, the instantaneous channel capacities are equal to the instantaneous mutual information seen at the destination and at the eavesdropper, respectively  $\mathcal{I}_D$  and  $\mathcal{I}_E$ , so that the instantaneous secrecy capacity is finally written as [4], [5]

$$\mathcal{C}_s = (\mathcal{I}_D - \mathcal{I}_E)^+. \quad (7)$$

From (7), it follows that the instantaneous secrecy capacity is positive when  $\gamma_D > \gamma_E$  and equal to zero when  $\gamma_D \leq \gamma_E$ . Thus, the probability of existence of a non-zero secrecy capacity is

$$\begin{aligned}\Pr\{\mathcal{C}_s > 0\} &= \Pr\{\gamma_D > \gamma_E\} \\ &= \int_0^\infty \int_0^{\gamma_D} p_{\gamma_D \gamma_E}(\gamma_D, \gamma_E) d\gamma_E d\gamma_D \\ &= \int_0^\infty \int_0^{\gamma_D} p_{\gamma_D}(\gamma_D) p_{\gamma_E}(\gamma_E) d\gamma_E d\gamma_D.\end{aligned}\quad (8)$$

Moreover, the *secrecy outage probability* (SOP) is the probability that  $\mathcal{C}_s$  is less than a target secrecy rate  $\mathcal{R}_s$  [5]:

$$\mathcal{S} = \Pr\{\mathcal{C}_s < \mathcal{R}_s\}. \quad (9)$$

For Rayleigh fading in the non-cooperative direct transmission (DT), the pdf and CDF of the random variable  $\gamma_D$  (the same holds to  $\gamma_E$ ) are given by [19]

$$F_{\gamma_D}(\gamma_D) = 1 - \exp\left(-\frac{\gamma_D}{\bar{\gamma}_D}\right), \quad (10a)$$

$$\begin{aligned}p_{\gamma_D}(\gamma_D) &= \frac{\partial [F_{\gamma_D}(\gamma_D)]}{\partial \gamma_D} \\ &= \frac{1}{\bar{\gamma}_D} \exp\left(-\frac{\gamma_D}{\bar{\gamma}_D}\right),\end{aligned}\quad (10b)$$

leading to the following probability of existence of non-zero secrecy capacity [4]

$$\Pr\{\mathcal{C}_{s,DT} > 0\} = \frac{\bar{\gamma}_D}{\bar{\gamma}_D + \bar{\gamma}_E}. \quad (11)$$

The SOP, in turn, was shown in [4] to be

$$\mathcal{S}_{DT}^{\text{csi}} = 1 - \frac{\bar{\gamma}_D}{\bar{\gamma}_D + 2^{\mathcal{R}} \bar{\gamma}_E} \exp\left(-\frac{2^{\mathcal{R}} - 1}{\bar{\gamma}_D}\right). \quad (12)$$

#### B. Sources without CSI

In this case we assume that the transmitters do not have CSI of either the legitimate or the eavesdropper channels. Thus, the instantaneous capacity seen at the legitimate destination,  $\mathcal{C}_D$ , is not known at the transmitters and therefore we must choose a fixed total number of  $2^{n\mathcal{R}}$  codewords and a fixed number of codewords per bin equal to  $2^{n\mathcal{R}_E}$  in the wiretap code. The fixed rate of attempted secure communication is

then  $\mathcal{R}_s = \mathcal{R} - \mathcal{R}_E$ . Therefore, an outage corresponds to the occurrence of any of the following two independent events [6]: i) The instantaneous channel capacity seen at the legitimate destination is smaller than  $\mathcal{R}$ . Such an event is referred to as *reliability outage* and has probability  $\Pr\{\mathcal{I}_D < \mathcal{R}\}$ ; ii) The instantaneous channel capacity seen at eavesdropper is larger than the equivocation rate  $\mathcal{R}_E$  of the wiretap code, so that the eavesdropper is able to recover at least part of the information intended to the legitimate transmitter. This event is referred to as *secrecy outage*, and has probability of occurrence given by  $\Pr\{\mathcal{I}_E \geq \mathcal{R}_E\}$ .

The overall secrecy outage probability is then given by the union of the two aforementioned independent events, being represented by

$$\begin{aligned} \mathcal{S}^{\text{no-csi}} &= \Pr\{(\mathcal{I}_D < \mathcal{R}) \cup (\mathcal{I}_E \geq \mathcal{R}_E)\} \\ &= \Pr\{\mathcal{I}_D < \mathcal{R}\} + \Pr\{\mathcal{I}_E \geq \mathcal{R}_E\} \\ &\quad - \Pr\{\mathcal{I}_D < \mathcal{R}, \mathcal{I}_E \geq \mathcal{R}_E\}. \end{aligned} \quad (13)$$

Generically, the secrecy outage probability of a given scheme  $X$  is obtained according to (13) as

$$\begin{aligned} \mathcal{S}_X^{\text{no-csi}} &= \mathcal{O}_X(\mathcal{R}, \bar{\gamma}_D) + [1 - \mathcal{O}_X(\mathcal{R}_E, \bar{\gamma}_E)] \\ &\quad - \mathcal{O}_X(\mathcal{R}, \bar{\gamma}_D) [1 - \mathcal{O}_X(\mathcal{R}_E, \bar{\gamma}_E)], \end{aligned} \quad (14)$$

where  $\mathcal{O}_X(\mathcal{R}, \bar{\gamma})$  is the reliability outage probability of scheme  $X$ .

For the direct transmission, through the substitution of (4) in (14), one can show that the SOP when the sources do not have any CSI is

$$\mathcal{S}_{\text{DT}}^{\text{no-csi}} = 1 - \exp\left(-\frac{2^{\mathcal{R}} - 1}{\bar{\gamma}_D}\right) \left[1 - \exp\left(-\frac{2^{\mathcal{R}_E} - 1}{\bar{\gamma}_E}\right)\right]. \quad (15)$$

#### IV. DECODE-AND-FORWARD (DF)

The decode-and-forward (DF) is a well established cooperative protocol, being largely investigated in recent works on cooperative communication, e.g. [10], [11], [13], [14]. In the DF protocol, after broadcasting their own IFs in the first time slot, each source retransmits a given partner's IF in the cooperative phase, usually adopting the same codebook (repetition code) as the source, as illustrated in Fig. 2(a) for a two-source network. Upon receiving two copies of the same message, the receiver performs maximum ratio combining (MRC) to optimally combine both observations. One can see that the code rate of DF is given by  $R_{\text{DF}} = 1/2$ , since one PF is transmitted in the cooperative phase for every IF broadcasted previously. Thus, in order to perform a fair comparison to the DT scheme, one must transmit with a transmission rate twice that of DT.

##### A. Sources with partial CSI

When the sources have CSI of the legitimate channels, the instantaneous secrecy capacity of the DF scheme is [10]

$$\mathcal{C}_{s,\text{DF}} = \frac{1}{2} \left( \log_2(1 + \gamma_D) - \log_2(1 + \gamma_E) \right)^+, \quad (16)$$

where  $\gamma_D$  and  $\gamma_E$  are respectively the instantaneous SNR at D and E after combining the messages. Assuming that the

channels between the sources are error-free<sup>1</sup> and focusing on the message of  $S_1$  (the same result is valid to the other source due to the symmetry), the instantaneous SNR seen at D and E after performing MRC is [19]

$$\begin{aligned} \gamma_D &= \bar{\gamma}_{1D} |h_{1D}|^2 + \bar{\gamma}_{2D} |h'_{2D}|^2, \\ &= \bar{\gamma}_D (|h_{1D}|^2 + |h'_{2D}|^2), \end{aligned} \quad (17a)$$

$$\begin{aligned} \gamma_E &= \bar{\gamma}_{1E} |h_{1E}|^2 + \bar{\gamma}_{2E} |h'_{2E}|^2, \\ &= \bar{\gamma}_E (|h_{1E}|^2 + |h'_{2E}|^2), \end{aligned} \quad (17b)$$

where the superscript ' refers to the channel realization in the cooperative phase ( $h_{iD}$  and  $h'_{iD}$  are assumed to be independent). From the results in [4], [13], it can be shown that the SOP of the two-source DF scheme in this case is

$$\begin{aligned} \mathcal{S}_{\text{DF}}^{\text{csi}} &= \Pr\{\mathcal{C}_{s,\text{DF}} < \mathcal{R}_s\} \\ &= 1 - \frac{\bar{\gamma}_D}{(\bar{\gamma}_D + \xi \bar{\gamma}_E)^3} \exp\left(-\frac{\xi - 1}{\bar{\gamma}_D}\right) \\ &\quad \times \left[ \bar{\gamma}_D (\xi - 1 + \bar{\gamma}_D) + \xi \bar{\gamma}_E (\xi - 1 + 3 \bar{\gamma}_D) \right], \end{aligned} \quad (18)$$

where  $\xi = 2^{2\mathcal{R}_s}$ .

##### B. Sources without CSI

When the sources do not have any CSI, the exact SOP of the two-source DF scheme is obtained from (14) as

$$\begin{aligned} \mathcal{S}_{\text{DF}}^{\text{no-csi}} &= \mathcal{O}_{\text{MRC}}(2\mathcal{R}, \bar{\gamma}_D) + [1 - \mathcal{O}_{\text{MRC}}(2\mathcal{R}_E, \bar{\gamma}_E)] \\ &\quad - \mathcal{O}_{\text{MRC}}(2\mathcal{R}, \bar{\gamma}_D) [1 - \mathcal{O}_{\text{MRC}}(2\mathcal{R}_E, \bar{\gamma}_E)] \\ &= 1 - \left[ 1 - \exp\left(-\frac{2^{2\mathcal{R}_E} - 1}{\bar{\gamma}_E}\right) \left[ 1 + \frac{2^{2\mathcal{R}_E} - 1}{\bar{\gamma}_E} \right] \right] \\ &\quad \times \exp\left(-\frac{2^{2\mathcal{R}} - 1}{\bar{\gamma}_D}\right) \left[ 1 + \frac{2^{2\mathcal{R}} - 1}{\bar{\gamma}_D} \right], \end{aligned} \quad (19)$$

where  $\mathcal{O}_{\text{MRC}}(\mathcal{R}, \bar{\gamma})$  corresponds to the 2-branch outage probability of the MRC scheme, which is given by [19]

$$\mathcal{O}_{\text{MRC}}(\mathcal{R}, \bar{\gamma}) = 1 - \exp\left(-\frac{2^{\mathcal{R}} - 1}{\bar{\gamma}}\right) \left[ 1 + \frac{2^{\mathcal{R}} - 1}{\bar{\gamma}} \right]. \quad (20)$$

#### V. NETWORK-CODED COOPERATION (NC)

In a non-binary network-coded (NC) based cooperative protocol with two sources, instead of just acting as routers, the sources are able to transmit linear combinations of all the available IFs during the cooperative phase, as illustrated in Fig. 2(b). If such linear combinations are performed over a high enough finite field, it is shown in [17] that gains in terms of diversity order can be achieved over the DF scheme.

Let us focus again on the message from  $S_1$  and focus for the moment being in the two-source case. If the intersource channel is not in outage (which happens with probability  $1 - \mathcal{O}(2\mathcal{R}, \bar{\gamma}_D)$ , where  $1 - \mathcal{O}(2\mathcal{R}, \bar{\gamma}_D)$  is the outage probability of an individual link obtained from (4)), we can see that D is able to recover  $S_1$ 's message from any two out the following four received frames:  $I_1$ ,  $I_2$ ,  $I_1 \boxplus I_2$ ,  $I_1 \boxplus 2I_2$  (the symbol  $\boxplus$  stands

<sup>1</sup>Note that this is an optimistic assumption that favors the DF scheme when compared to the other schemes. As our goal is to show that the network coding technique can outperform traditional cooperation protocols as DF, this assumption does not invalidate our results.



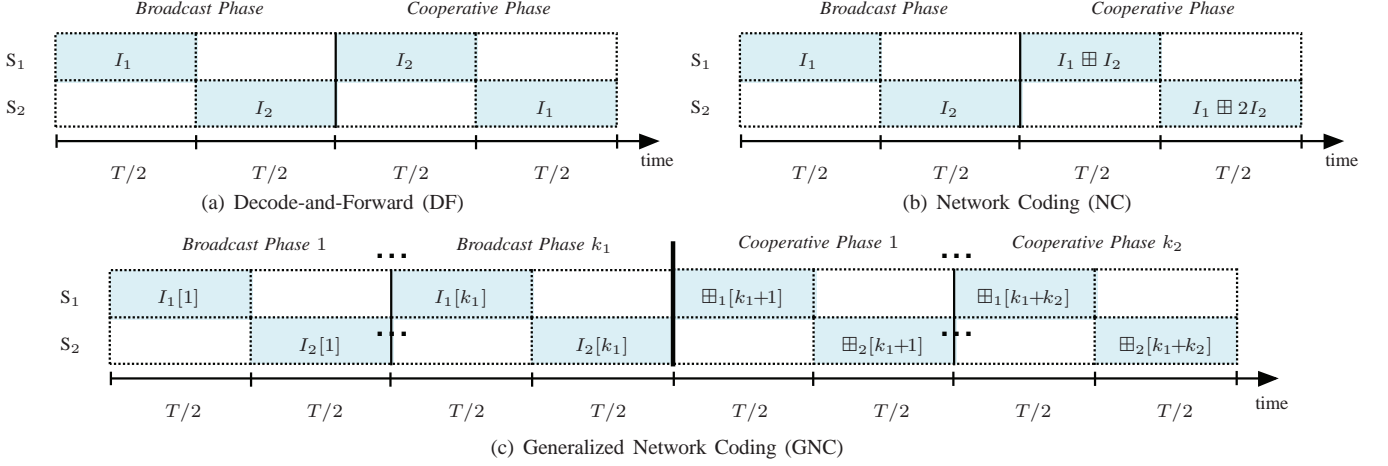


Fig. 2. Two-source time division channel allocation considering (a) Decode-and-Forward (DF) protocol; (b) Network Coding-based (NC) protocol; (c) Generalized Network Coding-based (GNC) protocol.  $T$  represents the time-slot duration and the symbol  $\oplus$  in (b) stands for summation over a finite field. In (c),  $\oplus_i[k]$  corresponds to a linear combination transmitted by source  $i$  at time slot  $k$ , which is composed of all the IFs received during the broadcast phase, including source's  $i$  own IFs.

for summation over a finite field). The information frame from  $S_1$  is not recovered by D when the direct transmission and at least two out of the three remaining packets cannot be decoded, which happens with probability [17]

$$\mathcal{O}_1(\mathcal{R}, \bar{\gamma}_D) \approx 3[\mathcal{O}(2\mathcal{R}, \bar{\gamma}_D)]^3. \quad (21)$$

When the channel between  $S_1$  and  $S_2$  is in outage (which happens with probability  $\mathcal{O}(2\mathcal{R}, \bar{\gamma}_D)$ ),  $S_1$  and  $S_2$  retransmit their own messages in the cooperative phase. Upon receiving two copies of the same message, we assume that D performs MRC, leading to the outage probability presented in (20).

The overall outage probability of the NC scheme was shown in [17] to be

$$\begin{aligned} \mathcal{O}_{\text{NC}}(\mathcal{R}, \bar{\gamma}_D) &= [1 - \mathcal{O}(2\mathcal{R}, \bar{\gamma}_D)] \mathcal{O}_1(\mathcal{R}, \bar{\gamma}_D) \\ &\quad + \mathcal{O}(2\mathcal{R}, \bar{\gamma}_D) \mathcal{O}_{\text{MRC}}(2\mathcal{R}, \bar{\gamma}_D) \\ &\approx 3.5 \left[ 1 - \exp\left(-\frac{2^{2\mathcal{R}} - 1}{\bar{\gamma}_D}\right) \right]^3, \end{aligned} \quad (22)$$

where the approximation holds for the high SNR region. We can see from (22) that diversity order of 3 is achieved, in contrast to the diversity order of 2 obtained by the DF scheme [17].

In [18], a generalization of the scheme proposed in [17] was presented, as illustrated in Fig. 2(c). In the scheme proposed in [18], referred to as generalized network coding (GNC), the sources are able to broadcast  $k_1$  IFs in the broadcast phase, as well as transmit an arbitrary number  $k_2$  of PFs in the cooperative phase, leading to a more flexible network code rate given by [18]

$$R_{\text{GNC}} = \frac{k_1}{k_1 + k_2}. \quad (23)$$

In this scenario with two sources, when the intersource channel is not in outage (which happens with probability  $1 - \mathcal{O}(\mathcal{R}/R_{\text{GNC}}, \bar{\gamma}_D)$ ), the destination receives  $2(k_1 + k_2)$  frames (each source broadcasts  $k_1$  IFs and then transmits  $k_2$  PFs in the cooperative phase), and a given IF is not recovered by D when the direct transmission and at least  $2k_2$  out of the remaining

$2(k_2 + k_1) - 1$  frames cannot be decoded, which happens with probability [18]

$$\mathcal{O}_1(\mathcal{R}, \bar{\gamma}_D) = \mathcal{O} \sum_{i=0}^{2k_1-1} \mu_{\text{GNC}_1}(i) \mathcal{O}^{2k_2+i} [1 - \mathcal{O}]^{2k_1-1-i}, \quad (24)$$

where  $\mathcal{O}$  is the short to  $\mathcal{O}(\mathcal{R}/R_{\text{GNC}}, \bar{\gamma}_D)$  and  $\mu_{\text{GNC}_1}(i) = \binom{2k_2+2k_1-1}{2k_2+i}$  corresponds to a binomial coefficient that takes into account the multiplicity of independent events that lead to the same outage probability.

When the intersource channel is in outage (which happens with probability  $\mathcal{O}_{12} = \mathcal{O}(\mathcal{R}/R_{\text{GNC}}, \bar{\gamma}_D)$ ), a given IF is not recovered by D when the direct transmission and at least  $k_2$  out of the  $k_2 + k_1 - 1$  remaining frames cannot be decoded, which happens with probability [18]

$$\mathcal{O}_2(\mathcal{R}, \bar{\gamma}_D) = \mathcal{O} \sum_{i=0}^{k_1-1} \mu_{\text{GNC}_2}(i) \mathcal{O}^{k_2+i} [1 - \mathcal{O}]^{k_1-1-i}, \quad (25)$$

where  $\mu_{\text{GNC}_2}(i) = \binom{k_2+k_1-1}{k_2+i}$ . The overall outage probability of the two-source GNC scheme is then given by:

$$\begin{aligned} \mathcal{O}_{\text{GNC}}(\mathcal{R}, \bar{\gamma}_D) &= (1 - \mathcal{O}_{12}) \mathcal{O}_1(\mathcal{R}, \bar{\gamma}_D) + \mathcal{O}_{12} \mathcal{O}_2(\mathcal{R}, \bar{\gamma}_D) \\ &= (1 - \mathcal{O}_{12}) \mathcal{O} \sum_{i=0}^{2k_1-1} \mu_1(i) \mathcal{O}^{2k_2+i} [1 - \mathcal{O}]^{2k_1-1-i} \\ &\quad + \mathcal{O}_{12} \mathcal{O} \sum_{i=0}^{k_1-1} \mu_2(i) \mathcal{O}^{k_2+i} [1 - \mathcal{O}]^{k_1-1-i}. \end{aligned} \quad (26)$$

#### A. Extension to the $M$ -source scenario

When the intersource channels are assumed to be outage-free, the outage probability of the  $M$ -source GNC scheme is obtained through the generalization of (24) as

$$\mathcal{O}_1(\mathcal{R}, \bar{\gamma}_D) = \mathcal{O} \sum_{i=0}^{Mk_1-1} \mu_{\text{GNC}_1}(i) \mathcal{O}^{Mk_2+i} [1 - \mathcal{O}]^{Mk_1-1-i}, \quad (27)$$

where  $\mu_{\text{GNC}_1}(i) = \binom{Mk_2+Mk_1-1}{Mk_2+i}$ . As presented in [18], the outage probability from (27) can be accurately approximated for the large SNR region as:

$$\mathcal{O}_{\text{GNC}}(\mathcal{R}, \bar{\gamma}_D) \approx \mu_{\text{GNC}_1} \left[ 1 - \exp \left( -\frac{2^{\mathcal{R}/R_{\text{GNC}}} - 1}{\bar{\gamma}_D} \right) \right]^{Mk_2+1}, \quad (28)$$

where  $\mu_{\text{GNC}_1} = \binom{Mk_2+Mk_1-1}{Mk_2}$ . Moreover, according to [18], when the intersource channels are subject to outages, the diversity is reduced and the approximation for the outage probability of a network with  $M$  sources operating under the GNC scheme with parameters  $(k_1, k_2)$  becomes

$$\tilde{\mathcal{O}}_{\text{GNC}}(\mathcal{R}, \bar{\gamma}_D) \approx \mu_{\text{GNC}_2} \left[ 1 - \exp \left( -\frac{2^{\mathcal{R}/R_{\text{GNC}}} - 1}{\bar{\gamma}_D} \right) \right]^{M+k_2}, \quad (29)$$

where  $\mu_{\text{GNC}_2} = \binom{k_1+k_2-1}{k_2}$ . From (29), it can be seen that the diversity order of the GNC scheme is  $M + k_2$ . By properly choosing the values of  $k_1$  and  $k_2$ , it can be shown that the GNC scheme can achieve both code rate and diversity order larger than the NC scheme. It is also worthy mentioning that the GNC scheme reduces to the NC scheme when  $k_1 = k_2 = 1$ .

Regarding the code design, the maximum diversity order of the GNC scheme is guaranteed if the coefficients of the linear combinations are chosen from a maximum distance separable (MDS) code<sup>2</sup> [18].

## VI. NETWORK-CODED COOPERATION WITH SECRECY CONSTRAINTS

In what follows we evaluate the SOP of the GNC scheme considering both the situations with partial CSI and without any CSI at the legitimate sources.

### A. Sources with partial CSI

In this situation, the sources know the legitimate channels and the SOP for the GNC scheme is obtained according to (9) as

$$\begin{aligned} \mathcal{S}_{\text{GNC}} &= \Pr \{ \mathcal{C}_{s,\text{GNC}} < \mathcal{R}_s \} \\ &= \Pr \left\{ R_{\text{GNC}} \left( \log_2(1 + \gamma_D) - \log_2(1 + \gamma_E) \right)^+ < \mathcal{R}_s \right\} \\ &= \Pr \left\{ \gamma_D < 2^{\mathcal{R}_s/R_{\text{GNC}}} (1 + \gamma_E) - 1 \right\} \\ &= \int_0^\infty \int_0^{\gamma_U} p_{\gamma_D, \gamma_E}(\gamma_D, \gamma_E) d\gamma_D d\gamma_E \\ &= \int_0^\infty \int_0^{\gamma_U} p_{\gamma_D}(\gamma_D) p_{\gamma_E}(\gamma_E) d\gamma_D d\gamma_E \\ &= \int_0^\infty F_{\gamma_D}(\gamma_U) p_{\gamma_E}(\gamma_E) d\gamma_E, \end{aligned} \quad (30)$$

where  $\gamma_U = 2^{\mathcal{R}_s/R_{\text{GNC}}} (1 + \gamma_E) - 1$ .

According to (30), in order to calculate the SOP, one must have the CDF of  $\gamma_D$  and the pdf of  $\gamma_E$ . The CDF is directly

obtained from the outage probability, whose exact value for a two-source GNC scheme is presented in (26), leading to

$$F_{\gamma_D}(\gamma_D) = \mathcal{O}_{\text{GNC}}(\mathcal{R}, \bar{\gamma}_D). \quad (31)$$

The pdf of  $\gamma_E$ , in turn, can be obtained by differentiating the outage probability (CDF) at the eavesdropper from (26):

$$p_{\gamma_E}(\gamma_E) = \frac{\partial [\mathcal{O}_{\text{GNC}}(\mathcal{R}_E, \bar{\gamma}_E)]}{\partial \gamma_E}. \quad (32)$$

Note that the exact outage probability in (26) is composed of several terms which results in a integration with multiple parts in (30) and finally in a long expression which leads to little insights. Besides that, (26) is restricted to the two-source case so that obtaining a generic closed-form exact expression is a tough task. Thus, in order to ease the analysis and the comprehension of the final results, in what follows we resort to (as will be shown shortly) a tight approximation through the following assumptions: *i)* We consider that the legitimate network is subject to outages in the intersource channels, so that the CDF of  $\gamma_D$  is approximated by (29); *ii)* The CDF of E is approximated by (28), which is an assumption that favors E, and makes the analysis more tractable, since the outages in the intersource channel do not depend on the rate  $\mathcal{R}_E$ , otherwise one would have to distinguish between the outages in the intersource channels and the outages in the direct channels when calculating the overall outage at E.

The CDF and pdf of  $\gamma_D$  are then approximated by<sup>3</sup>

$$F_{\gamma_D}(\gamma_D) \approx \left[ 1 - \exp \left( -\frac{\gamma_D}{\bar{\gamma}_D} \right) \right]^{M+k_2}. \quad (33a)$$

$$\begin{aligned} p_{\gamma_D}(\gamma_D) &= \frac{\partial [F_{\gamma_D}(\gamma_D)]}{\partial \gamma_D} \\ &\approx \frac{M+k_2}{\bar{\gamma}_D} \exp \left( -\frac{\gamma_D}{\bar{\gamma}_D} \right) \\ &\quad \times \left[ 1 - \exp \left( -\frac{\gamma_D}{\bar{\gamma}_D} \right) \right]^{M+k_2-1}. \end{aligned} \quad (33b)$$

The CDF and pdf of  $\gamma_E$ , in turn, are considered to be

$$F_{\gamma_E}(\gamma_E) \approx \left[ 1 - \exp \left( -\frac{\gamma_E}{\bar{\gamma}_E} \right) \right]^{Mk_2+1}. \quad (34a)$$

$$\begin{aligned} p_{\gamma_E}(\gamma_E) &= \frac{\partial [F_{\gamma_E}(\gamma_E)]}{\partial \gamma_E} \\ &\approx \frac{Mk_2+1}{\bar{\gamma}_E} \exp \left( -\frac{\gamma_E}{\bar{\gamma}_E} \right) \\ &\quad \times \left[ 1 - \exp \left( -\frac{\gamma_E}{\bar{\gamma}_E} \right) \right]^{Mk_2}. \end{aligned} \quad (34b)$$

By replacing the CDF and pdf of both  $\gamma_D$  and  $\gamma_E$  in (30), one can obtain an approximate expression for the SOP of the GNC scheme as presented in the following theorem.

<sup>3</sup>Note that  $\mu_{\text{GNC}_1}$  and  $\mu_{\text{GNC}_2}$  are made equal to one in (33) and (34) in order to limit the CDF and pdf to the unity and to have unity area, respectively, because the expressions in (29) and (28) are approximations for the high SNR and are not naturally limited to such values.

<sup>2</sup>Note that the MDS code is applied on the top of the Wiretap coding applied in the physical layer.

**Theorem 1.** *The SOP of the GNC scheme with partial CSI is approximated as*

$$\mathcal{S}_{\text{GNC}}^{\text{csi}} \approx (Mk_2 + 1) \sum_{i=0}^{M+k_2} \binom{M+k_2}{i} [-1]^i \exp\left(-\frac{\xi-1}{\bar{\gamma}_D} i\right) \times \text{B}\left(\frac{\xi \bar{\gamma}_E i + \bar{\gamma}_D}{\bar{\gamma}_D}, Mk_2 + 1\right), \quad (35)$$

where  $\xi = 2\mathcal{R}_s/R_{\text{GNC}}$  and  $\text{B}(x, y) = \int_0^1 t^{x-1} (1-t)^{y-1} dt$  corresponds to the Beta function (first order Euler function) [20].

*Proof:* Please refer to Appendix A.  $\square$

From Theorem 1, one can obtain the diversity order of the GNC scheme subjected to secrecy constraints as follows.

**Corollary 1.** *The diversity order of the  $M$ -source GNC scheme with parameters  $(k_1, k_2)$  is not reduced due to secrecy constraints, that is, it remains equal to  $M + k_2$ .*

*Proof:* Please refer to Appendix B.  $\square$

### B. Sources without CSI

When CSI is not available at the transmitter side, the exact SOP of the two-source GNC is obtained according to (14) after the substitution of  $\mathcal{O}_X(\mathcal{R}, \bar{\gamma}_D)$  and  $\mathcal{O}_X(\mathcal{R}_E, \bar{\gamma}_E)$  by the exact outage probability from (26). Similarly to the case with partial CSI, in order to make the analysis more tractable, we favor E here by considering that the outage probability experienced by E is obtained under the assumption of perfect intersource channels, that is,  $\mathcal{O}_X(\mathcal{R}_E, \bar{\gamma}_E)$  is dominated by the term  $\mathcal{O}_1(\mathcal{R}_E, \bar{\gamma}_E)$  in (26). Thus, the SOP of a two-source network operating under the GNC scheme is approximated by

$$\mathcal{S}_{\text{GNC}}^{\text{no-csi}} \approx \mathcal{O}_{\text{GNC}}(\mathcal{R}, \bar{\gamma}_D) + [1 - \mathcal{O}_1(\mathcal{R}_E, \bar{\gamma}_E)] - \mathcal{O}_{\text{GNC}}(\mathcal{R}, \bar{\gamma}_D)[1 - \mathcal{O}_1(\mathcal{R}_E, \bar{\gamma}_E)], \quad (36)$$

where  $\mathcal{O}_{\text{GNC}}(\mathcal{R}, \bar{\gamma}_D)$  and  $\mathcal{O}_1(\mathcal{R}_E, \bar{\gamma}_E)$  are obtained respectively from (26) and (24). Regarding its asymptotic behavior with the increase of  $\bar{\gamma}_D$ , the SOP from (36) presents a different behavior than the SOP of the GNC scheme with partial CSI from (35), as presented in the following Theorem.

**Theorem 2.** *When the SNR of the legitimate nodes increases without limit, the SOP of the GNC scheme presents an outage floor which is given by*

$$\begin{aligned} \bar{\mathcal{S}}_{\text{GNC}}^{\text{no-csi}} &= \lim_{\bar{\gamma}_D \rightarrow \infty} \mathcal{S}_{\text{GNC}}^{\text{no-csi}} \\ &\approx 1 - \mathcal{O}_1(\mathcal{R}_E, \bar{\gamma}_E). \end{aligned} \quad (37)$$

*Proof:* We can see from (4) that  $\mathcal{O}(\mathcal{R}, \bar{\gamma}_D) \rightarrow 0$  when  $\bar{\gamma}_D \rightarrow \infty$ . By replacing  $\mathcal{O}(\mathcal{R}, \bar{\gamma}_D) = 0$  in (14) and then in (36), one can see that the SOP is limited by the secrecy outage event ( $\mathcal{I}_E \geq \mathcal{R}_E$ ), whose probability of occurrence for the  $M$ -source GNC scheme obtained from the complement of (27) leads to (37), concluding the proof.  $\square$

In general, for the case of a  $M$ -source network, we can approximate the SOP from (36) by resorting to the high-SNR approximations of  $\mathcal{O}_{\text{GNC}}(\mathcal{R}, \bar{\gamma}_D)$  and  $\mathcal{O}_1(\mathcal{R}_E, \bar{\gamma}_E)$  given

respectively in (29) and (28), which leads to

$$\begin{aligned} \bar{\mathcal{S}}_{\text{GNC}}^{\text{no-csi}} &\approx 1 - \mu_{\text{GNC}_1} \left[ 1 - \exp\left(-\frac{2\mathcal{R}_E/R_{\text{GNC}} - 1}{\bar{\gamma}_E}\right) \right]^{Mk_2+1} \\ &\times \left[ 1 - \mu_{\text{GNC}_2} \left[ 1 - \exp\left(-\frac{2\mathcal{R}/R_{\text{GNC}} - 1}{\bar{\gamma}_D}\right) \right]^{M+k_2} \right]. \end{aligned} \quad (38)$$

However, as will be presented in the next section, even though the approximation from (38) is useful in obtaining an approximation to the slope of the SOP, it does not accurately represent the floor in the SOP according to (37). Thus, in what follows we present a more accurate approximation for the  $M$ -source GNC scheme than (38).

**Corollary 2.** *The SOP of the  $M$ -source GNC scheme can be approximated as*

$$\mathcal{S}_{\text{GNC}}^{\text{no-csi}} \approx \max \left\{ \bar{\mathcal{S}}_{\text{GNC}}^{\text{no-csi}}, \bar{\mathcal{S}}_{\text{GNC}}^{\text{csi}} \right\}, \quad (39)$$

where  $\bar{\mathcal{S}}_{\text{GNC}}^{\text{no-csi}}$  and  $\bar{\mathcal{S}}_{\text{GNC}}^{\text{csi}}$  are obtained from (37) and (38), respectively.

*Proof:* Since the approximation (38) does not reflect the actual behavior of the floor in the SOP, one can limit the SOP to the aforementioned floor by taking the maximum between the approximation in (38) and the asymptotic value from (37).  $\square$

## VII. NUMERICAL RESULTS

In this section, we present some numerical results in order to validate the results obtained analytically. For the GNC scheme, the instantaneous SNRs  $\gamma_D$  and  $\gamma_E$  were obtained according to the inverse transform sampling method [21]. In what follows, Figs. 3-6 refer to the case with partial CSI at the sources, while the scenario without any CSI at the sources is evaluated in Figs. 7-10. Unless stated otherwise, we assume the parameters  $M = k_1 = k_2 = 2$  for the GNC scheme, in order to perform a fair comparison to the DF scheme, such that the number of users and the code rate are the same.

Fig. 3 presents the SOP versus  $\bar{\gamma}_D$  for the DT, DF and GNC schemes, considering that  $\mathcal{R}_s = 0.5$  bits per channel use (bpcu) and that  $\bar{\gamma}_E = 10$  dB, as well as assuming CSI of the legitimate channels at the sources. For the GNC scheme in Fig. 3, “numerical” refers to the numerical result obtained from the exact SOP via Monte Carlo method, while “approx” refers to the analytical high-SNR approximation from (35). We can see that the GNC scheme presents the highest diversity order (slope of the curve) among all the three schemes, matching the value  $M + k_2 = 4$  (represented by the curve “asympt”) according to Corollary 1, which means that the GNC scheme outperforms the other schemes when a low SOP is required. It can also be seen that the numerical results match the analytical ones with good precision.

The influence of  $\bar{\gamma}_E$  in the SOP performance of the GNC scheme with partial CSI is evaluated in Fig. 4, considering that  $\mathcal{R}_s = 0.5$  bpcu and  $\bar{\gamma}_E = \{5, 10, 15\}$  dB. We can see that when  $\bar{\gamma}_E$  increases, the SOP performance is degraded in terms

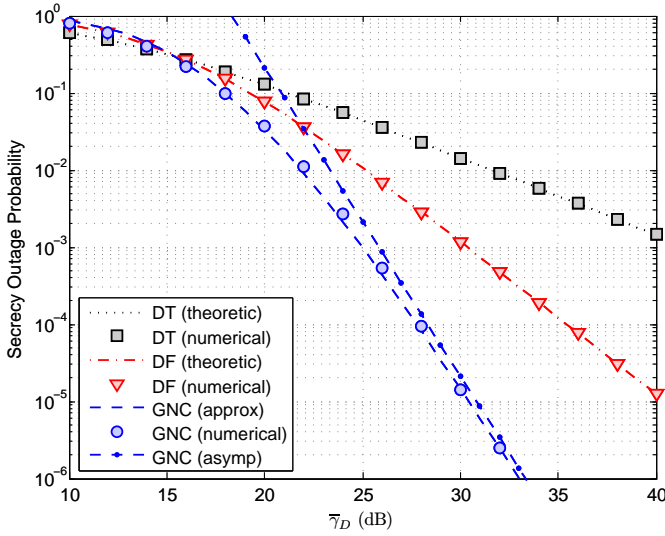


Fig. 3. Secrecy outage probability versus  $\bar{\gamma}_D$  for the DT, DF and GNC schemes (with  $M = k_1 = k_2 = 2$ ), considering  $\mathcal{R}_s = 0.5$  bpcu and Eve's average SNR  $\bar{\gamma}_E = 10$  dB. Partial CSI scenario.

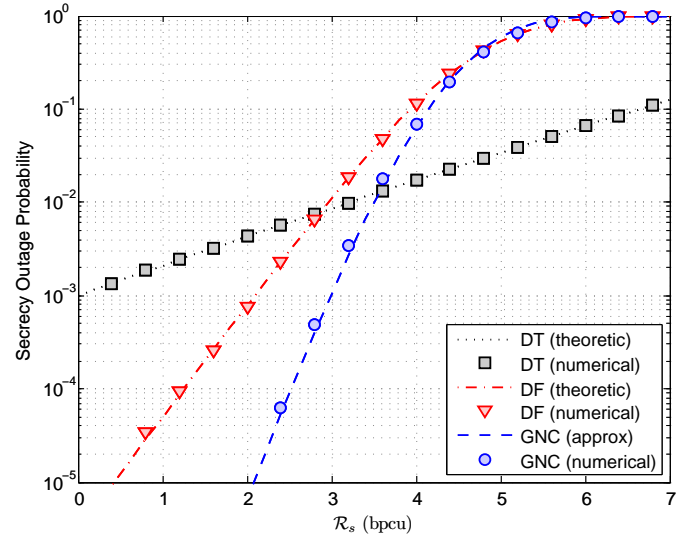


Fig. 5. Secrecy outage probability versus  $\mathcal{R}_s$  for DT, DF and GNC (with  $M = k_1 = k_2 = 2$ ) schemes, considering  $\bar{\gamma}_D = 40$  dB and  $\bar{\gamma}_E = 10$  dB. Partial CSI scenario.

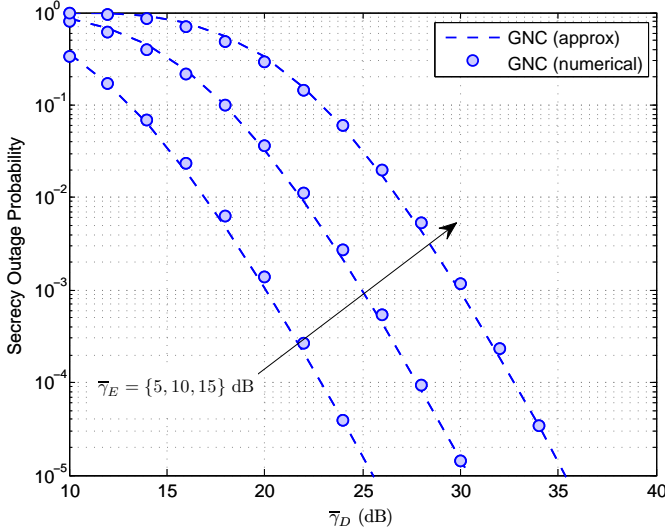


Fig. 4. Secrecy outage probability versus  $\bar{\gamma}_D$  for GNC scheme (with  $M = k_1 = k_2 = 2$ ), considering  $\mathcal{R}_s = 0.5$  bpcu and Eve's average SNR  $\bar{\gamma}_E = \{5, 10, 15\}$  dB. Partial CSI scenario.

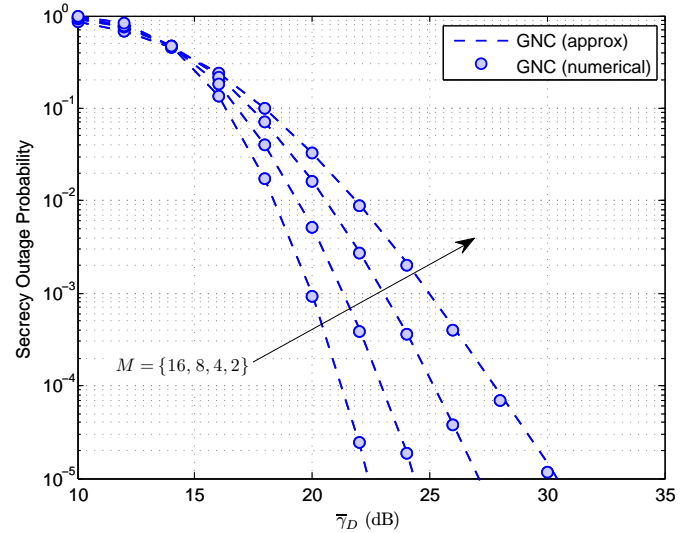


Fig. 6. Secrecy outage probability versus  $\bar{\gamma}_D$  for GNC scheme (with  $k_1 = k_2 = 2$ ), considering  $\mathcal{R}_s = 0.5$  bpcu,  $\bar{\gamma}_E = 10$  dB and  $M = \{2, 4, 8, 16\}$ . Partial CSI scenario.

of coding gain (the curve is moved to the right). However, the diversity order remains unchanged.

Fig. 5 evaluates the SOP of the DT, DF and GNC schemes with partial CSI as a function of the secrecy rate  $\mathcal{R}_s$ . One can see that the cooperative schemes outperform the DT up to a certain threshold of  $\mathcal{R}_s$ , from which the DT presents the lowest SOP. However, for the low-SOP region, the GNC scheme is the one that presents the best performance.

The SOP versus  $\bar{\gamma}_D$  for the GNC scheme with different numbers of sources  $M$  is presented in Fig. 6. We can see that the performance of the scheme, as its diversity order, increases as the number of users increases. However, the relative gains diminish with the increase of  $M$ .

Fig. 7 considers the case without CSI at the sources, and

shows the SOP versus  $\bar{\gamma}_D$  for the situation where  $\mathcal{R} = 3$  bpcu,  $\mathcal{R}_E = 2$  bpcu and  $\bar{\gamma}_E = 2$  dB. In Fig. 7, “theoretic” refers to the SOP obtained from (36), “approx” refers to the approximation in (38) and “asympt” to the asymptotic result according to (37). One can see that all the considered schemes present an error floor which is limited by the secrecy outage event, however, the floor of the GNC scheme is the lowest. It is also worth noting that the exact SOP is well approximated by the maximum between the approximated and the asymptotic results from (39), Corollary 2.

The influence of  $\bar{\gamma}_E$  in the SOP performance in the case without CSI is evaluated in Fig. 8, for the DT, DF and GNC schemes with  $\mathcal{R} = 3$  bpcu,  $\mathcal{R}_E = 2$  bpcu and  $\bar{\gamma}_D = 30$  dB. One can see that the GNC scheme presents



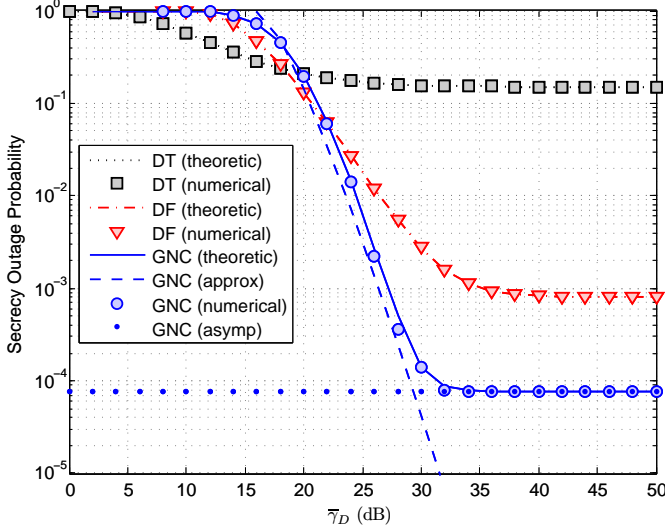


Fig. 7. Secrecy outage probability versus  $\bar{\gamma}_D$  for the DT, DF and GNC (with  $M = k_1 = k_2 = 2$ ) schemes without CSI at the transmitters, considering  $\mathcal{R} = 3$  bpcu,  $\mathcal{R}_E = 2$  bpcu and Eve's average SNR  $\bar{\gamma}_E = 2$  dB. No CSI scenario.

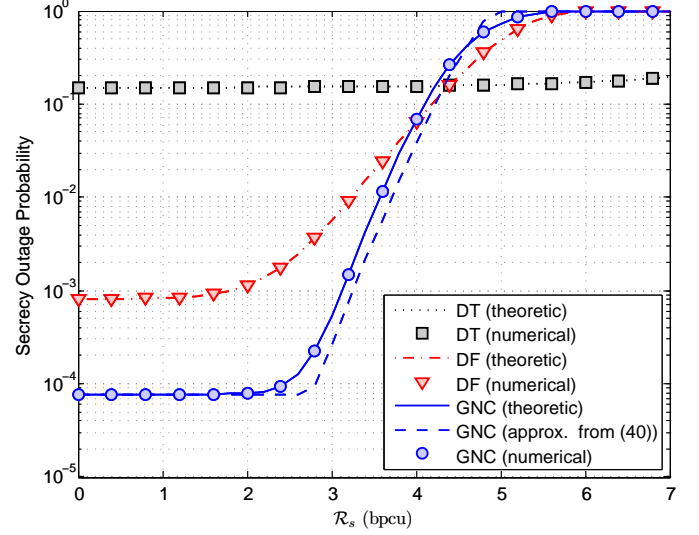


Fig. 9. Secrecy outage probability versus  $\mathcal{R}_s$  for the DT, DF and GNC (with  $M = k_1 = k_2 = 2$ ) schemes, considering  $\mathcal{R}_E = 2$  bpcu,  $\bar{\gamma}_E = 2$  dB and  $\bar{\gamma}_D = 40$  dB. No CSI scenario.

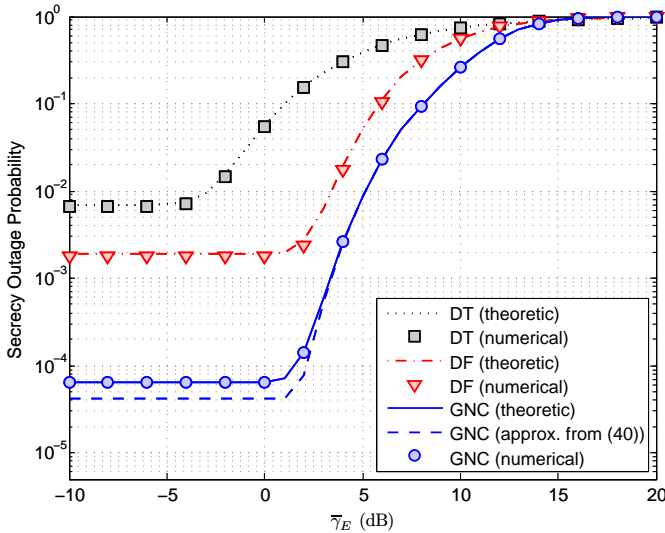


Fig. 8. Secrecy outage probability versus  $\bar{\gamma}_E$  for the DT, DF and GNC (with  $M = k_1 = k_2 = 2$ ) schemes without CSI at the transmitters, considering  $\mathcal{R} = 3$  bpcu,  $\mathcal{R}_E = 2$  bpcu and  $\bar{\gamma}_D = 30$  dB. No CSI scenario.

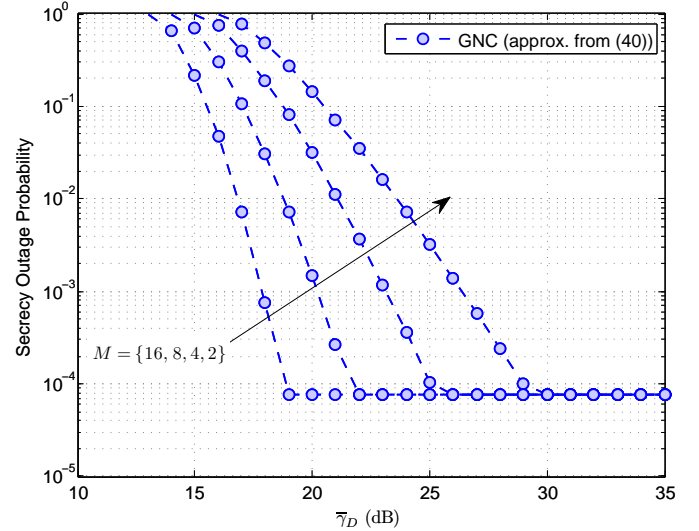


Fig. 10. Secrecy outage probability versus  $\bar{\gamma}_D$  for the GNC scheme (with  $k_1 = k_2 = 2$ ), considering  $\mathcal{R} = 3$  bpcu,  $\mathcal{R}_E = 2$  bpcu,  $\bar{\gamma}_E = 2$  dB and  $M = \{2, 4, 8, 16\}$ . No CSI scenario.

the lowest SOP for the whole considered range. It can also be seen that the approximation from (39) is useful in obtaining an approximation for the SOP of the GNC scheme.

Fig. 9 evaluates the influence of the secrecy rate  $\mathcal{R}_s$  on the performance of the DT, DF and GNC schemes, considering that  $\mathcal{R}_E = 2$  bpcu,  $\bar{\gamma}_E = 2$  dB and  $\bar{\gamma}_D = 40$  dB. We can see that the SOP of all schemes increase when  $\mathcal{R}_s$  increases. However, the GNC is the scheme that presents the lowest SOP in the region of low SOP.

Fig. 10 presents the SOP versus  $\bar{\gamma}_D$  for the GNC scheme with different numbers of sources  $M$ . We can see that the performance of the scheme is improved as the number of users increases. However, besides the relative gains diminish with

the increase of  $M$ , one can see that the floor in the SOP is approximately the same, independently of  $M$ . This is due to the fact that the floor corresponds to the complement of the outage probability so that its variation is only noticeable at the high SOP range.

## VIII. FINAL COMMENTS

We evaluated the secrecy outage probability of a multi-source cooperative network where the destination node is wiretapped by a malicious and passive eavesdropper. We proposed the application of the network coding technique as an alternative to increase the secrecy at the destination node. Different scenarios with partial and completely without channel state information (CSI) at the sources were evaluated

and we showed through theoretic and numerical analyses that the secrecy can be significantly increased through the use of network coding when compared to the direct transmission and traditional cooperative techniques.

#### APPENDIX A PROOF OF THEOREM 1

*Proof:* After replacing the CDF of  $\gamma_D$  obtained from (33a) and the pdf of  $\gamma_E$  obtained from (34b) in (30), we have that:

$$\begin{aligned} \mathcal{S}_{GNC}^{\text{csi}} &= \int_0^\infty F_{\gamma_D}(\gamma_U) p_{\gamma_E}(\gamma_E) d\gamma_E \\ &\approx \frac{Mk_2+1}{\bar{\gamma}_E} \int_0^\infty \overbrace{\left[1 - \exp\left(-\frac{\gamma_U}{\bar{\gamma}_D}\right)\right]^{M+k_2}}^{\mathbf{A}} \\ &\quad \times \exp\left(-\frac{\gamma_E}{\bar{\gamma}_E}\right) \left[1 - \exp\left(-\frac{\gamma_E}{\bar{\gamma}_E}\right)\right]^{Mk_2} d\gamma_E. \end{aligned} \quad (40)$$

We then expand term **A** in (40) using the binomial expansion

$[1-x]^n = \sum_{i=0}^n \binom{n}{i} [-1]^i x^i$ , leading to:

$$\begin{aligned} \mathcal{S}_{GNC}^{\text{csi}} &\approx \frac{Mk_2+1}{\bar{\gamma}_E} \int_0^\infty \sum_{i=0}^{M+k_2} \binom{M+k_2}{i} [-1]^i \exp\left(-\frac{\gamma_U}{\bar{\gamma}_D} i\right) \\ &\quad \times \exp\left(-\frac{\gamma_E}{\bar{\gamma}_E}\right) \left[1 - \exp\left(-\frac{\gamma_E}{\bar{\gamma}_E}\right)\right]^{Mk_2} d\gamma_E. \end{aligned} \quad (41)$$

According to [20, eq. (3.312.1)], one has that:

$$\int_0^\infty \left[1 - \exp\left(-\frac{x}{\beta}\right)\right]^{\nu-1} \exp(-\alpha x) dx = \beta B(\beta\alpha, \nu). \quad (42)$$

Thus, by substituting  $\gamma_U = \xi(1 + \gamma_E) - 1$  in (41) and substituting in (42)  $\beta = \bar{\gamma}_E$ ,  $\nu = Mk_2 + 1$ , and  $\alpha = (\xi\bar{\gamma}_E i + \bar{\gamma}_D)/(\bar{\gamma}_D \bar{\gamma}_E)$ , we can obtain (35), concluding the proof.  $\square$

#### APPENDIX B PROOF OF COROLLARY 1

*Proof:* According to the definition of diversity order presented in (6), one must evaluate the asymptotically behavior of the outage probability with respect to  $\bar{\gamma}_D$ . For large values of  $\bar{\gamma}_D$ , the Beta function from (35) can be approximated as [20]:

$$\begin{aligned} B\left(\frac{\xi\bar{\gamma}_E i + \bar{\gamma}_D}{\bar{\gamma}_D}, Mk_2+1\right) &\approx B(1, Mk_2+1) \\ &= \frac{\Gamma(1)\Gamma(Mk_2+1)}{\Gamma(Mk_2+2)} \\ &= \frac{1}{Mk_2+1}, \end{aligned} \quad (43)$$

where  $\Gamma(\cdot)$  corresponds to the complete Gamma function [20]. Thus, by replacing (43) in (35), one have that:

$$\begin{aligned} \mathcal{S}_{GNC}^{\text{csi}} &\approx [Mk_2+1] \sum_{i=0}^{M+k_2} \binom{M+k_2}{i} [-1]^i \exp\left(-\frac{\xi-1}{\bar{\gamma}_D} i\right) \\ &\quad \times \left[\frac{1}{Mk_2+1}\right] \\ &= \sum_{i=0}^{M+k_2} \binom{M+k_2}{i} [-1]^i \exp\left(-\frac{\xi-1}{\bar{\gamma}_D} i\right). \end{aligned} \quad (44)$$

After resorting to the fact that  $\sum_{i=0}^n \binom{n}{i} [-1]^i x^i = [1-x]^n$ , the SOP from (44) can be rewritten as

$$\mathcal{S}_{GNC}^{\text{csi}} \approx \left[1 - \exp\left(-\frac{\xi-1}{\bar{\gamma}_D}\right)\right]^{M+k_2}. \quad (45)$$

Finally, the diversity order  $M + k_2$  from Corollary 1 is obtained by applying (45) in (6).  $\square$

#### REFERENCES

- [1] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, pp. 656–715, 1949.
- [2] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.
- [3] P. K. Gopala, L. Lai, and H. El-Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct 2008.
- [4] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. of the IEEE Int. Symp. on Inform. Theory (ISIT'06)*, 2006.
- [5] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*, C. U. Press, Ed. Cambridge University Press, 2011.
- [6] X. Tang, R. Liu, and P. Spasojevic, "On the achievable secrecy throughput of block fading channels with no channel state information at transmitter," in *41st Annual Conference on Information Sciences and Systems, 2007. (CISS '07)*, March 2007, pp. 917–922.
- [7] X. Tang, R. Liu, P. Spasojevic, and H. Poor, "On the throughput of secure hybrid-arq protocols for gaussian block-fading channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 4, pp. 1575–1591, April 2009.
- [8] H. Alves, R. D. Souza, M. Debbah, and M. Bennis, "Performance of transmit antenna selection physical layer security schemes," *IEEE Signal Process. Lett.*, vol. 19, no. 6, pp. 372–375, June 2012.
- [9] N. Yang, P. L. Yeoh, M. El-kashlan, R. Schober, and I. B. Collings, "Transmit antenna selection for security enhancement in MIMO wiretap channels," *IEEE Trans. Commun.*, vol. 61, no. 1, pp. 144–154, January 2013.
- [10] F. Gabry, "Cooperation for secrecy in wireless networks," Ph.D. dissertation, KTH, School of Electrical Engineering, Communication Theory Laboratory, September 2012.
- [11] L. Lai and H. E. Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4005–4019, September 2008.
- [12] R. Kaido, O. K. Rayel, J. L. Rebelatto, and R. D. Souza, "Network coded cooperation for a two-user wiretap channel," in *Proc. of the IEEE Int. Conf. on Acoustics, Speech and Signal Processing (ICASSP'14)*, Florence, Italy, May 2014.
- [13] J. N. Laneman, D. N. C. Tse, and G. W. Wornell, "Cooperative diversity in wireless networks: Efficient protocols and outage behavior," *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 3062–3080, December 2004.
- [14] A. Sendonaris, E. Erkip, and B. Aazhang, "User cooperation diversity: Part I and Part II," *IEEE Trans. Commun.*, vol. 51, no. 11, pp. 1927–1948, November 2003.
- [15] E. C. van der Meulen, "Three-terminal communication channels," *Advanced Applied Probability*, vol. 3, pp. 120–154, 1971.
- [16] R. Ahlswede, N. Cai, S.-Y. Li, and R. Yeung, "Network information flow," *IEEE Trans. Inf. Theory*, vol. 46, no. 4, pp. 1204 – 1216, 2000.

- [17] M. Xiao and M. Skoglund, "Multiple-user cooperative communications based on linear network coding," *IEEE Trans. Commun.*, vol. 58, no. 12, pp. 3345–3351, December 2010.
- [18] J. L. Rebelatto, B. F. Uchôa-Filho, Y. Li, and B. Vucetic, "Multi-user cooperative diversity through network coding based on classical coding theory," *IEEE Trans. Signal Process.*, vol. 60, no. 2, pp. 916–926, February 2012.
- [19] A. Goldsmith, *Wireless Communications*. Cambridge University Press, 2005.
- [20] I. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 7th ed., A. Jeffrey and D. Zwillinger, Eds. Academic Press - Elsevier, 2007.
- [21] L. Devroye, *Non-Uniform Random Variate Generation*, Springer-Verlag, Ed. New York: Springer-Verlag, 1986.